

Hotlines in France: CNIL Publishes Application Documents

FEBRUARY 2006

The Network developed this update regarding the CNIL Decision working with our legal counsel to offer suggestions based on our experience and knowledge of best practices. We encourage all organizations to work with their legal counsel on this or any other matter regarding legal compliance.

OVERVIEW

The CNIL has published Single Authorization Number AU-004 in order to simplify the hotline application process for organizations utilizing an employee hotline in France. If your organization complies with the articles of this Decision, a simple declaration form can be filed in lieu of the more extensive application process. Otherwise the organization will need to apply using the full application process. *A translation of the key points of the Single Authorization Decision follows this analysis.*

The major concerns of businesses seeking to comply with both CNIL and Sarbanes-Oxley have been resolved:

- The Decision allows for acceptance of anonymous reports, so long as the investigation of anonymous allegations follows specific guidelines (See Article 2)
- Although the hotline scope should be limited to financial irregularities, reports about other matters of "critical concern" or involving workplace safety may be accepted
- The CNIL has specifically accepted the use of third-party providers outside of France if they are Safe Harbor Certified.

The declaration form is available in French at <http://www.cnil.fr/index.php?id=1758>

Guidance on the full application process is available in French at http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/declarer-CNIL.pdf

COMPLIANCE ISSUES

The twelve articles of the Single Authorization Decision focus on several broad categories. At a high level, compliance involves:

- Communication to employees
- Investigation procedures
- Processes for destruction of records
- Processes for handling calls

ISSUE: EMPLOYEE COMMUNICATION. Communication to French employees must include specific information:

- The name of the person or department responsible for the hotline, the hotline's purpose and the scope of issues that can be reported via the hotline
- Information about the organization that answers calls and whether calls are answered outside of the EU
- A statement that employees are not required to use the hotline and that there will be no adverse consequence to employees who do not use the hotline
- An explanation of the right of any person identified in a report to access and correct information
- A statement that abuse of the hotline may expose the employee to disciplinary sanctions, but good faith use will not result in discipline

ISSUE: INVESTIGATION. The CNIL requires that the accused party be notified of the allegation. The timing of notification is supposed to be rapid, but notification does not need to happen until investigators have secured evidence that might otherwise be at risk. A review of investigation processes should be undertaken to address how and when notification of the accused party would be accomplished.

ISSUE: DATA RETENTION/DESTRUCTION. Compliance requires that records of personal information, such as the names of the caller and the accused party, be destroyed two months after the conclusion of the investigation, if no disciplinary or legal action is underway. This requirement pertains to records held by a hotline provider or by the employer in any database, case management system or any hard copy files. If the report concerns a matter outside of the scope of the hotline's stated purpose, the record is to be destroyed immediately.

ISSUE: HOTLINE INTERVIEW PROCESS. The CNIL requirements have implications in two areas:

- Limiting the scope of reports accepted regarding French operations
- Modifying interviews to enforce the scope and discourage anonymous reports

Scope of the Hotline

Although the CNIL wants the hotline to be primarily available for reporting financial irregularities, it makes an exception for other reports of vital concern to the organization or threatening the physical or emotional safety of its employees (See Article 3).

NEXT STEPS: Ensure your hotline provider has a process for identifying reports from France and enforcing the limited scope. Work with legal counsel to determine the list of codes. Consider incidents that would typically warrant immediate notification, which seems to be the spirit of the exception described in the Decision.

Possible Incident Codes

- Accounting/Audit Irregularities and other Sarbanes-Oxley codes
- Discrimination/Harassment
- Fraud-related codes
- Product Quality Concern
- Substance Abuse
- Workplace Violence/Threats

MORE INFORMATION

If you have questions about any of the above information, please contact The Network at 800-357-5137 or send an email to info@tnwinc.com.

Single Authorization Decision

The Single Authorization Decision allows businesses wishing to implement hotlines that conform to the following articles to simply send CNIL a commitment to comply with the Decision. They receive a receipt acknowledging their statement by return mail and may then implement their hotline. If certain conditions are met, this also serves as authorization to transfer data to countries outside of the European Union. The commitment form is available at <http://www.cnil.fr/index.php?id=1758>

If the process is not in compliance with these 12 articles, the authorization procedure requires the filing of a complete application dossier, which must be examined in a plenary session of the Commission within two months of filing, provided no additional information is needed. Guidance on the complete application process in French is available at http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/declarer-cnil.pdf

ARTICLE 1. SCOPE OF THE PROCEDURE

Only those hotlines which are for the purpose of addressing a legal or regulatory obligation regarding the internal control of financial, accounting, banking or anti-corruption matters, are in conformity with this decision.

Procedures adopted to comply with Section 301(4) of the American Sarbanes-Oxley Act of July 2002 are within the scope of the present decision.

ARTICLE 2. TREATMENT OF THE CALLER'S IDENTITY

The caller should identify himself, but the organization managing the hotline must keep his identity confidential.

The organization may only accept an anonymous call under the following conditions:

- the investigation of the report must be handled with every precaution
- a preliminary investigation must be undertaken before disseminating the report to others in the organization
- The organization should discourage anonymous calls in any communications about the hotline. The procedure should be set up to assume that all callers will identify themselves.

ARTICLE 3. TYPES OF PERSONAL DETAILS THAT CAN BE RECORDED

Only the following details can be recorded:

- the identity, job and location of the caller
- the identity, job and location of the person who is the subject of the call
- the identity, job and location of the individuals involved in the receipt or investigation of the report
- the facts reported
- evidence gathered in the course of investigating the report

- report of the investigation
- outcome of the report

The facts gathered are limited to those relating to subject matter within the scope of the hotline. Facts relating to other subjects may only be passed on to the appropriate people within the organization when they concern a vital interest of the organization, or the physical or moral safety of the workforce.

The final report must be based only on objectively formulated information directly related to the subject of the call, and strictly necessary to its investigation. The language used to describe third party statements should make clear that these are allegations.

ARTICLE 4. DISSEMINATION OF PERSONAL DETAILS

Those charged within the organization with the receipt or investigation of hotline calls should only have access to as much of the personal details described in Article 3. as needed to be able to fulfill their function.

These details should only be communicated outside the organization to individuals charged with the management of the hotline in other divisions or units of the company if necessary to investigate the call or its consequences for the group.

If a third party provider is employed to receive or handle hotline calls, the individuals responsible at the third party provider should have access only to those personal details described in Article 3. which allow them to fulfill their specific role. The third party provider must contractually undertake not to use these details for any other purpose, to assure their confidentiality, to respect the limited data retention period, and to destroy or hand over all electronic or manual records at the end of the contract term.

In all cases, the individuals involved in the receipt and investigation of hotline calls should be strictly limited in number, receive specialized training, and be subject to a stringent, contractually-defined duty of confidentiality.

ARTICLE 5. TRANSFER OF PERSONAL DETAILS OUTSIDE THE EUROPEAN UNION

This article applies to cases where the dissemination described in Article 4. involves a transfer of information to entities located in a country that is not a member of the European Union, and therefore not covered by Article 68 of the Law of January 6, 1978, as amended.

In such cases, all communications of personal details must be made in conformity with the January 6, 1978, Law, in particular, Article 69, paragraph 8.

This requirement is satisfied if the entity where the person receiving the details works adheres to Safe Harbor, and has included these types of data within its Safe Harbor certification.

It is also satisfied if the destination entity has a contract which includes the clauses established by the CNIL in its decisions of June 15, 2001, or December 27, 2004, or when the company of which the concerned organization or entities form a part has had internal rules approved in advance by the CNIL as guaranteeing a sufficient level of protection to individual privacy and fundamental rights. If these conditions are satisfied and if the transfer complies with all the other requirements of this decision, the transfer will be deemed to comply with Article 69, paragraph 8 of the Law of January 6, 1978, as amended.

ARTICLE 6. RECORD RETENTION PERIODS FOR PERSONAL DETAILS

Any details considered outside the scope of the hotline program should be destroyed or archived immediately, subject to the next to last paragraph of Article 3, if applicable.

Where the hotline report has been investigated, the details should be destroyed two months after the conclusion of the investigation, provided that the investigation is not followed by disciplinary or judicial action.

When discipline is imposed, or judicial action undertaken against the person named in the call, or against a caller who has abused the hotline program, the details should be retained until proceedings are concluded.

ARTICLE 7. SECURITY MEASURES

The person responsible should take all useful precautions to preserve the security of the details whether regarding their receipt, communication or retention.

In particular, access to details should be restricted to those with a user ID and individual password, regularly updated, or by other authentication methods. Access should be recorded and regularly monitored.

The identity of a caller must be treated confidentially so as to prevent the caller experiencing retaliation for his action.

ARTICLE 8. NOTICE TO POTENTIAL CALLERS

Potential users of the hotline should receive clear and complete information about it.

In addition to the collective and individual information required by the Labor Code, and in compliance with Article 32 of the Law of January 6, 1978, as amended, information about the hotline should identify precisely the entity responsible for the hotline, its purpose and scope, the optional character of the hotline, no adverse consequence to employees who do not use the hotline, where calls go to, whether

details are transferred outside the European Union, as well as the right of any person identified in a call to access and correct information.

It must be clearly stated that abuse of the hotline may expose the caller to disciplinary sanctions, as well as judicial proceedings, but, on the other hand, the good faith use of the hotline, even if the facts are later found to be incorrect or inconclusive, will not expose the caller to disciplinary action.

ARTICLE 9. NOTICE TO THOSE NAMED IN HOTLINE CALLS

A person named in a hotline call must be informed of the details of the call by the person responsible for the hotline program as soon as they are recorded, or at least of those details which would allow him to defend himself in an investigation.

When conservation measures are necessary, for example, to prevent the destruction of evidence, the person named in the call need not be informed until after these measures have been taken.

Information to the person named will specify the entity responsible for the hotline program, the allegations against him, the persons who might be informed about the call, as well as how to exercise his rights to access and correct the information. If the person has not yet been given the information required under Article 8, he should also be given that.

ARTICLE 10. RESPECT FOR RIGHTS OF ACCESS AND CORRECTION

In compliance with Articles 39 and 40 of the Law of January 6, 1978, as amended, the person responsible for the hotline program guarantees to anyone named in a call the right to access the personal details concerning him, and, if they are incorrect, incomplete, equivocal, or out of date, to correct or delete them.

A person named in a hotline call may not obtain the identity of the person who made the call.

ARTICLE 11

Any hotline program which includes the handling of personal details and which does not conform to the preceding requirements must be approved by the CNIL following the procedure prescribed by Articles 25-1 4 and 30 of the January 6, 1978 Law, as amended.

ARTICLE 12

This decision will be published in the Official Journal of the French Republic.



ReportLine™

NetClaim™

mPower Communications®

FOR MORE INFORMATION CALL 800.357.5137 OR VISIT WWW.REPORTLINE.NET